US Operation Choke Point dogged by controversy

Operation Choke Point has received a significant amount of criticism, which reached a head after a financial services trade association moved to sue federal bank regulators, accusing the agencies of improperly issuing and enforcing new policies that prevent banks from handling transactions for payday lenders and other 'high risk' online merchants. Allyson B. Baker and Thomas E. Gilbertsen of Venable LLP, analyse the concerns and the extent to which a party can be held liable for another's conduct.

The US Department of Justice ('DOJ') leads a posse of state and federal financial agencies that comprise the Financial Fraud Enforcement Task Force's Consumer Protection Working Group. In this capacity, the DOJ is now riding the range in search of banks and payment processors that handle transactions for 'outlaws' in the Wild West of internet based commerce. Dubbed 'Operation Choke Point,' the initiative is sparking controversy as it seeks to hold banks and other payment processors accountable for perceived misdeeds of their merchant customers. Earlier this year, the DOJ brought its first civil suit under the Operation, suing a North Carolina community bank and alleging that it willfully ignored violations of consumer laws by online payday lenders who were customers of a payment processor with accounts at the bank. On the same day the DOJ filed suit in *United States v. Four Oaks Bank & Trust Co.*, it also submitted a consent decree for court approval, in which the bank agreed to pay a $1.2 million penalty under the Financial Institutions Reform, Recovery and Enforcement Act ('FIRREA') and implement tighter controls over internet based merchants with accounts at the bank. Since January 2013, the DOJ has reportedly served about 50 subpoenas on banks and payment processors as part of this initiative, and recently announced that prosecutors in the DOJ's Consumer Protection Branch are finalising more complaints against banks as the Operation moves forward.

The Operation is drawing an extraordinary amount of flak from industry groups, trade press and some Congressional leaders. The stated concerns are threefold. First, the Operation appears to be sweeping too broadly and impacting lawful merchant activity. It is not yet clear how much of this may be unintended consequences but, in response to the Operation, entire categories of internet merchants are becoming *persona non grata* in the nation's banks, cutting some merchants off from automated payment systems and putting billion dollar sectors like online payday lending at risk of extinction. Secondly, law enforcement and bank regulatory officials are pursuing third party liability theories that seek to hold these financial institutions accountable for unproven allegations about the lawfulness of bank customer conduct. Third, some argue the Operation amounts to rulemaking by enforcement action - a course of action that may circumvent constitutional due process and violate statutes prohibiting arbitrary regulatory rules.

The affected online merchants operate in a number of so-called 'high risk' areas that get increasing scrutiny from payment systems like NACHA, card networks, regulators and law enforcement. Online payday lenders get all the ink, but many other internet marketers are now tagged as 'high risk' by payment networks and regulators. 'High risk' categories include not just palpable scams and Ponzi schemes, but a long list of otherwise lawful products and services that are heavily regulated by state or federal law. Some examples of high risk merchant activities include ammunition sales, credit repair and debt settlement services, gambling, nutritional supplements, tobacco sales...even 'legal services' have been identified as high risk. Recent guidance from the Federal Deposit Insurance Corporation ('FDIC') emphasises that high risk activities are typically characterised by high return rates and high rates of unauthorised transactions, as well as consumer complaints and indications of regulatory or law enforcement actions against participating merchants. And because these online transactions rely on credit cards, remotely created cheques, demand drafts, and ACH debit transactions, they present heightened risks of post-sale unauthorised transactions.

The Operation is being challenged by trade groups in court and in Congress. A financial services trade association recently sued federal bank regulators in a Washington DC federal court, accusing the agencies of improperly issuing and enforcing new policies that effectively prevent banks from handling transactions for payday lenders and other 'high risk' online merchant categories. Meanwhile, some in Congress are pressing the DOJ and bank regulators for more transparency, criticising a 'shoot now, ask questions later' approach that threatens entire categories of online merchant activity without directly challenging, let alone proving, that the underlying merchants violated any laws.

Given the sad history of

consumer fraud in the internet marketplace and the challenges it presents to law enforcement and the payments industry, the Operation can come as no surprise. Focus on a 'choke point' has been building for years as industry groups, payment networks and government agencies scouted for ways to combat unauthorised transactions and cut off fraudulent merchants from access to electronic payment systems. But the internet is a challenging range to police. Industry groups like NACHA and credit card networks have promulgated rules requiring member banks to conduct due diligence of merchant clients, monitoring their marketing activities and reporting or suspending merchants whose monthly transactions exceed stated thresholds for unauthorised and other types of returns. Yet, some merchants prove remarkably adept at avoiding detection. Over the years, state attorneys general and the Federal Trade Commission ('FTC') have expended substantial resources in court battles against individuals behind fraudulent internet marketing schemes, but these Sisyphean efforts have seemingly little impact in an internet marketplace characterised by ease of entry and few accountability safeguards.

Legal obstacles also dog law enforcement attempts to hold third party payment processors and banks responsible for the misdeeds of account holders. 'Accomplice' liability always comes down to a question of degree. As one seminal decision observes, "many variables enter into the equation on how much aid is 'substantial aid' sufficient to invoke liability." *Halberstam v. Welch*, 705 F.2d 472, 483 (D.C. Cir. 1983). At one end of the spectrum, a party is liable for another's conduct when they participate in a conspiracy by committing a tortious act furthering the primary wrongdoer's goals. At the other extreme, mere 'presence at the scene' of wrongdoing is insufficient to establish liability. This is the widely-accepted Restatement of Torts approach, for which courts identify five factors: (i) nature of the act that the defendant encouraged; (ii) amount and kind of assistance defendant gave; (iii) defendant's absence or presence at time of underlying wrongdoing; (iv) defendant's relation to the tortious actor; and (v) defendant's state of mind such as knowledge of falsity, willful ignorance.

The limits of accomplice liability can hamper FTC enforcement in this arena because that agency lacks aiding and abetting jurisdiction under Section 5 of the FTC Act

The limits of accomplice liability can hamper FTC enforcement in this arena because that agency lacks aiding and abetting jurisdiction under Section 5 of the FTC Act. See *Central Bank of Denver N.A. v. First Interstate Bank of Denver*, 511 U.S. 164 (1994). Nor does the FTC have jurisdiction over banks, which are subject to supervisory jurisdiction from a variety of federal and state bank regulators, as well as enforcement jurisdiction from these same bank regulators and the DOJ. Although bank regulators wield credible enforcement tools *viz.* the banks they regulate, they often lack effective authority over payment processors and merchants. But in a recent action alleging deceptive marketing practices by a bank customer involved in student loan servicing, the Federal Reserve obtained a consent decree providing $4.1 million civil money penalties, restitution up to $30 million, and a consent order limiting the bank from working with third parties that solicit, market or service consumer deposit products. See *In re Cole Taylor Bank* (Fed. Reserve Brd. of Governors 26 June 2014). The Federal Reserve's action reached both bank and merchant by alleging that they met the test for institution affiliated parties and that the underlying services were subject to Federal Reserve regulation and examination under the Bank Service Act.

With its Operation, the DOJ is now exercising FIRREA and Anti-Fraud Injunction Act authority against banks in a way that is turning heads. The DOJ relies heavily on FIRREA, which allows civil penalties for violations of 14 different federal criminal laws. So under FIRREA, the DOJ need only rely on a civil burden of proof when alleging underlying criminal conduct. See 12 U.S.C. § 1833a(f). Some of these provisions, including the most commonly alleged predicates of mail and wire fraud, require that the challenged conduct must 'affect' federally insured financial institutions. See 12 U.S.C. §1833a. FIRREA also provides a ten year statute of limitations, and gives the DOJ administrative subpoena authority.

Prospects for a court resolving the Operation's controversies are not encouraging. As closely regulated, government chartered financial institutions that rely on the good graces of their regulators, banks are unlikely to go the distance against the DOJ in FIRREA litigation. At press time, two Congressional hearings about the Operation are pending in the House Judiciary and Financial Services Committees. But legislative solutions are hard to come by these days. The solution must come from the banking and law enforcement agencies themselves, as all affected parties agree that a more carefully calibrated approach is necessary.

Allyson B. Baker Partner
Thomas E. Gilbertsen Partner
Venable LLP, Washington DC
tegilbertsen@Venable.com
abbaker@Venable.com